Kevin Laukaitis (NJ Bar ID # 155742022)
LAUKAITIS LAW FIRM LLC
737 Bainbridge Street #155
Philadelphia, PA 19147
Phone: 215-789-4462
Email: klaukaitis@laukaitislaw.com

Attorneys for Plaintiff and the Proposed Classes

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

SHEN BEI, individually on behalf of himself and on behalf of all others similarly situated,

Plaintiff,

v.

BetMGM, LLC.,

Defendant.

Case No. _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Shen Bei ("Plaintiff") brings this Class Action Complaint ("Complaint") against BetMGM, LLC ("MGM" or "Defendant"), as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff brings this Complaint against MGM for its failure to properly secure and safeguard the personally identifiable information that it collected and maintained as part of its regular business practices, including, but not limited to: full names; contact information; dates of birth; Social Security numbers; and other sensitive information (collectively, "personally identifiable information" or "PII").

2. Defendant is "the exclusive sports betting division of MGM, both online and in MGM casinos nationwide."[1]

3. Upon information and belief, former and current MGM consumers are required to entrust Defendant with sensitive, non-public PII, which Defendant could not perform its regular business activities without, in order to place a wager with MGM. Defendant apparently retains this information for at least many years—even after the consumer relationship has ended.

4. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. On November 28, 2022, Defendant became aware of suspicious activity on its networks (the "Data Breach"). Upon discovering the suspicious activity, Defendant "promptly launched an investigation" and determined that "certain BetMGM patron records were obtained in an unauthorized manner", which Defendant "believe[s] . . . occurred in May 2022."

6. According to Defendant's Important Notice About Your Personal Information letter (the "Notice Letter"), the compromised PII included individuals' full names; contact information; dates of birth; Social Security numbers; and other sensitive, non-public information.

7. Although only MGM is yet to disclose the number of customers impacted by the security breach to attorney generals, the PII compromised in the Data Breach included Plaintiff's and up to 1.5 million other individuals' information.

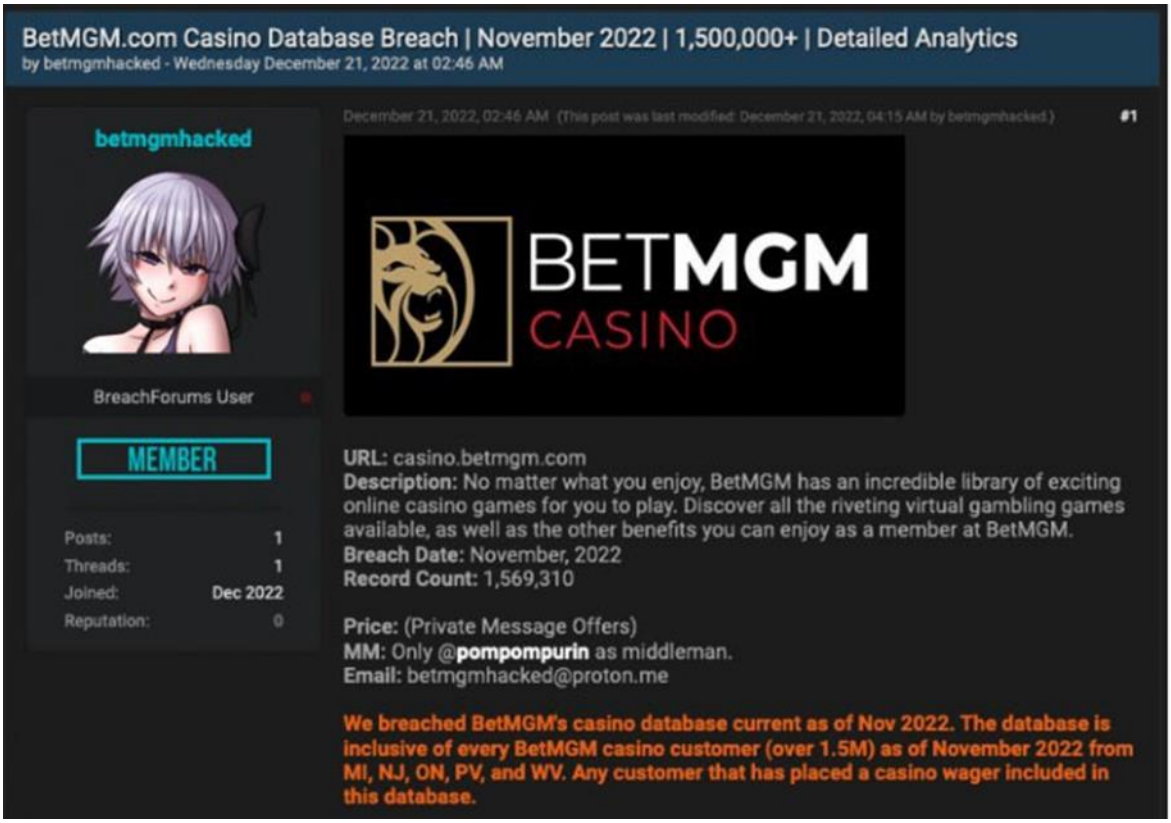
8. Although only MGM is yet to disclose the number of customers impacted by

[1] https://www.betmgminc.com/who-we-are/.

the security breach to attorney generals, the PII compromised in the Data Breach included Plaintiff's and up to 1.5 million other individuals' information.

9. Security Week, a cybersecurity publication, reports that on December 21, 2022, a cybercriminal posted an offer to a database containing all 1.57 million customer records that were stolen from MGM and further boasted that:[2]

> We breached BetMGM's casino database current as of Nov 2022. The database is inclusive of every BetMGM casino customer (over 1.5M) as of November 2022 from MI, NJ, ON, PV, and WV. Any customer that has placed a casino wager included in this database.



[2] https://www.securityweek.com/betmgm-confirms-breach-hackers-offer-sell-data-15-million-customers

10. Defendant failed to adequately protect Plaintiff's and Class Members PII—and failed to even encrypt or redact this highly sensitive information. Had this information been properly encrypted, the cybercriminals would have made off with only unintelligible data. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect customers' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members. Indeed, the cybercriminals that perpetrated the hack are already attempting to sell it on dark web forums. This present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

11. Moreover, Defendant failed to provide Plaintiff and Class Members with timely and adequate notice. The Data Breach occurred in "May 2022" and was detected by Defendant on November 28, 2022, yet Defendant did not notify impacted customers until December 21, 2022. During this time, Plaintiff and Class Members were unaware that their sensitive PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

12. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

13. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

14. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

15. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.[3]

16. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and, the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

17. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

PARTIES

18. Plaintiff Shen Bei is a resident and citizen of the state of New York, currently residing in Nyak, New York. Plaintiff was notified of the Data Breach and his PII being compromised via receiving the Notice Letter directly from Defendant, via E-mail dated December 21, 2022.[4]

19. Defendant BetMGM, LLC describes itself as a "partnership between MGM Resorts International and Entain Holdings that is revolutionizing sports betting and online gaming in the United States,"[5] and is incorporated under the laws of the state of New Jersey, with its principal office located at Harborside Plaza 2, 200 Hudson Street, Suite 700, Jersey City, New Jersey 07311.[6] Upon information and belief, the citizenship of Defendant's LLC's members is New Jersey.

---

[3] The Montana Attorney General Office reported that 225 Montana residents were impacted in the Data Breach. See https://dojmt.gov/consumer/databreach/

[4] All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

[5] https://www.betmgminc.com/who-we-are/

[6] https://www.njportal.com/DOR/businessrecords/EntityDocs/BusinessStatCopies.aspx

20. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

COMMON FACTUAL ALLEGATIONS

MGM's Business

21. Defendant is a New Jersey-based sports betting and online gambling company, formed by "a partnership between MGM Resorts International and Entain Holdings".[7] Defendant currently operates in over twenty countries and is the "exclusive sports betting division of MGM."[8]

22. Plaintiff and Class Members are current or former MGM customers.

23. To place a bet or wager at MGM, Plaintiff and Class Members were required to provide sensitive and confidential PII, including their names, dates of birth, Social Security numbers, financial information, and other sensitive information.

24. Defendant required that Plaintiff and Class Members create an account and provide PII as a condition of using Defendant's services.

25. The information held by Defendant in its computer systems included the unencrypted PII of Plaintiff and Class Members.

26. Upon information and belief, Defendant made promises and representations to its customers, including Plaintiff and Class Members, that the PII collected from them as a condition of creating a MGM account (and required to place bets) would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

[7] https://www.betmgminc.com/who-we-are/
[8] Id.

27. Indeed, the Privacy Policy posted on Defendant's website includes sections on "How we protect your data" and "What data breach procedures we have in place".[9]

28. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

29. Plaintiff and the Class Members value, and have taken reasonable steps to maintain, the confidentiality of their PII. Plaintiff and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

30. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer's PII safe and confidential.

31. Defendant had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

32. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

[9] https://sports.betmgm.com/en/blog/privacy-policy/

BetMGM's Data Breach

34. On or about December 21, 2022, Defendant began sending Plaintiff and other victims of the Data Breach a Notice Letter, informing them that:

> We are writing to notify you of an issue that involves certain of your personal information. We have learned that certain BetMGM patron records were obtained in an unauthorized manner. We believe that your information was contained in these records, which may have included details such as name, contact information (such as postal address, email address and telephone number), date of birth, hashed Social Security number, account identifiers (such as player ID and screen name) and information related to your transactions with us. The affected information varied by patron.
>
> We promptly launched an investigation after learning of the matter and have been working with leading security experts to determine the nature and scope of the issue. We learned of the issue on November 28, 2022, and believe the issue occurred in May 2022. We currently have no evidence that patron passwords or account funds were accessed in connection with this issue. Our online operations were not compromised. We are coordinating with law enforcement and taking steps to further enhance our security.

35. Omitted from the Notice Letter were the exact date of the Data Breach's occurrence, why it took MGM approximately six months to detect the Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, the information specific to individuals that was compromised in the Data Breach, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

36. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

37. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

38. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted PII of Plaintiff and Class Members, including their names, contact information, dates of birth, Social Security numbers. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

39. Plaintiff further believes his PII, and that of Class Members, was subsequently offered for sale on the dark web following the Data Breach, as, not only is that the *modus operandi* of cybercriminals that commit cyber-attacks of this type, but a hacker has apparently posted a database of 1,569,310 BetMGM records for sale on the dark web.[10]

40. Plaintiff's and Class Members' PII also could also fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

Data Breaches Are Preventable

41. As the Federal Bureau of Investigation explains, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[11]

42. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

[10] https://www.bleepingcomputer.com/news/security/leading-sports-betting-firm-betmgm-discloses-data-breach/

[11] See How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 23, 2021).

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[12]

43. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs)

[12] Id. at 3-4.

have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[13]

44. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full

[13] See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at: https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Oct. 17, 2022).

compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface]for Office [Visual Basic for Applications].[14]

45. Given that Defendant was storing the sensitive PII of its current and former customers, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

46. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of thousands of customers, including that of Plaintiff and Class Members.

Defendant Acquires, Collects, and Stores Its Customers' PII

47. As a condition to create an account and place a bet or wager at MGM, Plaintiff and

[14] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Nov. 11, 2021).

Class Members were required to give their sensitive and confidential PII to Defendant. Plaintiff and Class Members provided their PII with the expectation and mutual understanding that Defendant would safeguard their PII against foreseeable threats.

48. Defendant retains and stores this information and derives a substantial economic benefit from the PII that it collects. But for the collection of Plaintiff's and Class Members' PII, Defendant would be unable to provide its gambling services.

49. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

50. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

51. Defendant could have prevented this targeted Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members.

52. Upon information and belief, Defendant made promises to Plaintiff and Class Members to maintain and protect PII, demonstrating an understanding of the importance of securing PII.

Defendant Knew Or Should Have Known Of The Risk Because Gambling Companies In Possession Of PII Are Particularly Susceptible To Cyber Attacks

53. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

54. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store PII and other sensitive information, like Defendant, preceding the date of the breach.

55. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[15]

56. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[16]

57. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

58. Additionally, as companies became more dependent on computer systems to run their business[17], e.g., working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[18]

59. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiff and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed

[15] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.
[16] Id.
[17] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html.
[18]https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022.

on Plaintiff and Class Members as a result of a breach.

60. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

61. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."

62. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

63. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to over 1.5 million individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

64. In the Notice Letter, Defendant makes an offer of 24 months of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII. Moreover, once this service expires, Plaintiff and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

65. Defendant's offering of credit and identity monitoring establishes that Plaintiff's and Class Members' sensitive PII *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

66. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

67. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

68. As a gambling company in custody of current and former customers' PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

PII is Very Valuable

69. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[19] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

[19] 17 C.F.R. § 248.201 (2013).

70. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[20] For example, Personal Information can be sold at a price ranging from $40 to $200.[21] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[22]

71. For example, Social Security numbers, which were compromised for Plaintiff and some Class Members as alleged herein, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[23]

[20] Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Oct. 17, 2022).
[21] Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian, Dec. 6, 2017, available at: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 17, 2022).
[22] In the Dark, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 217, 2022).
[23] Social Security Administration, Identity Theft and Your Social Security Number, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Oct. 17, 2022).

72. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

73. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[24]

74. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number and name.

75. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[25]

76. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

[24] Bryan Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015), available at: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Oct. 17, 2022).

[25] Tim Greene, Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, IT World, (Feb. 6, 2015), available at: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 17, 2022).

77. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[26]

78. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

Defendant Fails to Comply With FTC Guidelines

79. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

80. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

[26] Report to Congressional Requesters, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited Oct. 17, 2022).

81. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[27]

82. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

83. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

84. These FTC enforcement actions include actions against resort companies that offer sports gambling to customers, like Defendant. *See, e.g., In re Marriot Int'l, Inc. Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 481 (D. Md. 2020) (Plaintiffs' claim, alleging a violation of Section 5 FTC Act, was adequately pleaded "based on. . . appellate court decisions. . . interpreting Section 5 of the FTC Act, and. . . federal court decisions finding [a viable claim] based on the Section 5 FTC Act in data breach cases[.])

[27] Id.

85. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

86. Defendant failed to properly implement basic data security practices.

87. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to its customers' PII or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

88. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the PII of its customers. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

Defendant Also Fails to Comply With Basic Industry Standards

89. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

90. Several best practices have been identified that a minimum should be implemented by gambling companies in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus,

and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

91. Other best cybersecurity practices that are standard in the gambling industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including by failing to train staff.

92. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

93. These foregoing frameworks are existing and applicable industry standards in gambling industry, and upon information and belief, Defendant failed to comply with at least one––or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Common Injuries and Damages

94. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals,

the risk of identity theft to the Plaintiff and Class Members have materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) the loss of benefit of the bargain (price premium damages); (e) diminution of value of their Private Information; and (f) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

Data Breaches, like Defendant's Here, Increase An Individual's Risk of Identity Theft

95. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information, precisely as they have done here. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

96. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

97. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to

manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victims.

Loss Of Time To Mitigate The Risk Of Identity Theft And Fraud

98. As a result of the recognized risk of identity theft, when a Data Breach occurs and an individual is notified by a company that their PII was compromised, as here, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet the resource and asset of time has been lost.

99. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, as the Notice Letter encourages them to do, monitor their financial accounts for many years to mitigate the risk of identity theft.

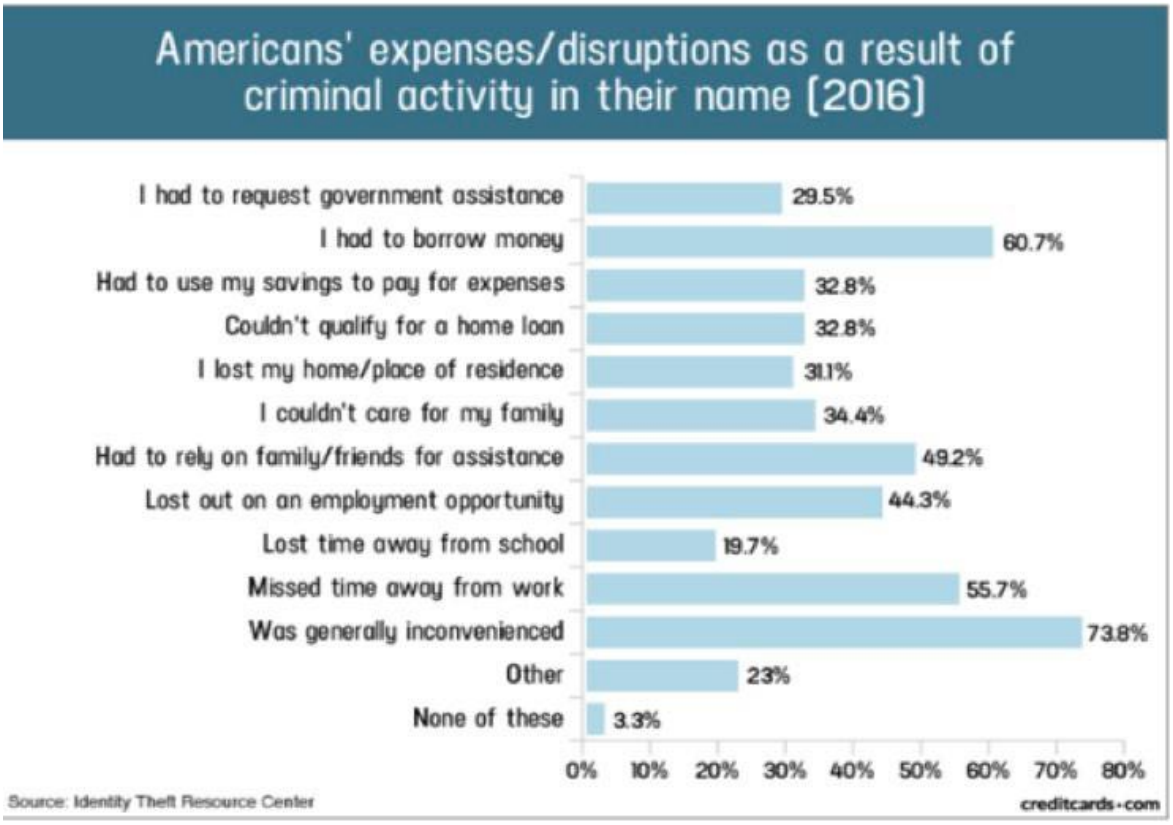
100. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such contacting financial institutions, closing or modifying financial accounts, signing up for credit and identity theft monitoring insurance; and monitoring credit reports and accounts for unauthorized activity, which may take years to discover and detect.

101. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[28]

[28] See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

102. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[29]

103. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[30]



[29] See Federal Trade Commission, Identity Theft.gov, https://www.identitytheft.gov/Steps (last visited July 7, 2022).

[30] Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Sep 13, 2022).

104. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[31]

Diminution Of Value Of PII

105. PII is a valuable property right.[32] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

106. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other entities in custody of healthcare and medical information often purchase PII on the black market for the purpose of target marketing their products and services to the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PII to adjust their insureds' medical insurance premiums.

107. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[33]

108. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[34] In fact, the data marketplace is so

[31] See "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Sep. 13, 2022) ("GAO Report").
[32] See, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[33] Ashiq Ja, Hackers Selling Healthcare Data in the Black Market, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sep. 13, 2022).
[34] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[35,36] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[37]

109. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

110. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

111. The fraudulent activity resulting from the Data Breach may not come to light for years.

112. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

[35] https://datacoup.com/
[36] https://digi.me/what-is-digime/
[37] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

113. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Credit And Identity Theft Monitoring Is Reasonable & Necessary

114. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and reports of dissemination on the dark web, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

115. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

116. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[38]

117. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

[38] See Jesse Damiani, Your Social Security Number Costs $4 On The Dark Web, New Report Finds, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

118. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

Loss Of Benefit Of The Bargain

119. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to provide their PII under certain terms in order to create a MGM account (as required to place wagers at MGM), Plaintiff and other reasonable consumers understood and expected that they were, in part, paying, or being paid less, for services and data security to protect the PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Mr. Bei's Experience with Defendant and the Data Breach

120. Plaintiff Bei is an MGM customer. When he originally created his MGM account in approximately July 2022 while he was still living in New Jersey, Plaintiff Bei was required to provide extensive amounts of his PII to MGM, including his name, date of birth, contact information, and Social Security number.

121. Defendant retained Plaintiff's PII in its system.

122. Plaintiff Bei is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

123. Plaintiff Bei received the Notice Letter directly from MGM via E-mail, dated December 21, 2022. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties. This sensitive information included Plaintiff's name, date of birth, contact information, and Social Security number.

124. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach and has spent time and effort on this mitigation, and Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

125. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (a) diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

126. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

127. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

128. Plaintiff Bei has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

129. Plaintiff brings this class action on behalf of himself and on behalf of all others similarly situated, pursuant to the Federal Rules of Civil Procedure 23, for the following Classes defined as:

Nationwide Class:

All individuals residing in the United States whose PII was compromised in the data breach first announced by Defendant on or about December 21, 2022 (the "Nationwide Class").

New York Subclass:

All individuals residing in the State of New York whose PII was compromised in the data breach first announced by Defendant on or about December 21, 2022 (the "New York Subclass").

New Jersey Subclass:

All individuals residing in the State of New Jersey whose PII was compromised in the data breach first announced by Defendant on or about December 21, 2022 (the "New Jersey Subclass").

130. Unless otherwise stated herein, the classes listed above shall be referred to as the "Class."

131. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

132. Plaintiff reserves the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

133. **Numerosity**: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. Upon information and belief, at least multiple thousand individuals were notified by Defendant of the Data Breach.

Moreover, the Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

134. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

k. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and,

l. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

138. **Typicality:** Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

139. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

140. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages he has suffered are typical of

other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

141. **Superiority and Manageability:** The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

142. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

143. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

144. Adequate notice can be given to Class Members directly using the information maintained in Defendant's records.

145. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

146. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

147. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and,

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members.

CAUSES OF ACTION

COUNT I

NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

148. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully alleged herein.

149. Defendant required Plaintiff and Class Members to submit non-public Personally Identifiable Information including, but not limited to, full names, dates of birth, contact information and Social Security Numbers, as a condition of gambling at MGM.

150. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

151. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiff and the Classes in Defendant's possession was adequately secured and protected.

152. By assuming the responsibility to collect and store this data, and in fact doing so, and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it— to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

153. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of creating a gambling account at MGM, and because Defendant was in an exclusive position to maintain the confidentiality of their PII.

154. Defendant's duty to use reasonable care in protecting confidential data arose also because Defendant is bound by industry standards to protect confidential PII.

155. Defendant also had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair. . . practices in or

affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

156. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII they were no longer required to retain pursuant to regulations.

157. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Class as a result of the reasonably foreseeable likelihood of a targeted data breach.

158. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

159. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiff and the Class, including basic encryption techniques, freely available to Defendant.

160. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

161. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully accessed by an unauthorized third party as a result of the Data Breach.

162. Plaintiff and the Class had no ability to protect their PII that was in, and likely remains in, Defendant's possession.

163. The imposition of a duty of care on Defendant to safeguard the PII it maintained is appropriate because any social utility of Defendant's conduct—of which there is little, if any to—is outweighed by the injuries suffered by Plaintiff and Class Members as a result of the Data Breach.

164. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and the Class's PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard the Class's PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Class Members' PII;

d. Failing to detect in a timely manner that Class Members' PII had been compromised; and,

e. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

165. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members, particularly because of the known high frequency of cyberattacks and data breaches in the industry.

166. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

167. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

168. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) their financial accounts and funds within such being frozen; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Class; and (vii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

169. As a direct and proximate result of Defendant' negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not

limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

170. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

171. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT II

NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Nationwide Class)

172. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully alleged herein.

173. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

174. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

175. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se.*

176. Plaintiff and the Class Members are within the class of individuals that the FTC Act seeks to protect. The FTC Act expressly prohibits "unfair" acts that "cause or are likely to cause substantial injury to consumers which is not reasonably avoidable by consumers."

177. Additionally, the harm that has occurred to Plaintiff and the other Class Members is the type of harm the FTC Act were intended to prevent and remedy. FTC authorities have pursued a number of enforcement actions against businesses that caused the unauthorized dissemination, collection or use of their customers' Private Information and personal information as a result of the businesses' lack of reasonable and adequate security measures and practices.

178. But for Defendant's negligence *per se*, breach of its duties, and/or negligent supervision of its agents, contractors, vendors, and suppliers, Plaintiff and the Class Members would not have suffered injury-in-fact. The injury and harm suffered by Plaintiff and the Class Members was the reasonably foreseeable result of, and directly traceable to, Defendant's breach of its duties. Defendant knew or should have known that they were failing to meet their duties, and that Defendant's breach thereof would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

179. As a direct, actual, and proximate result of Defendant's negligent and/or negligence *per se* conduct, Plaintiff and Class Members have suffered injuries including, but not limited to: (i) their financial accounts and funds within such being frozen; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching

how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Class; and (vii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

180. Plaintiff and Class Members have been injured and are entitled to damages.

COUNT III

BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class)

181. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully alleged herein.

182. Defendant required Plaintiff and the Class to provide their personal information, including name, address, date of birth, contact information, and Social Security number, as a condition of gambling at MGM.

183. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

184. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

185. Had Plaintiff and Class Members known that Defendant would not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

186. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal and financial information and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the data breach.

187. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) injuries including, but not limited to: (i) their financial accounts and funds within such being frozen; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Class; and (vii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

COUNT IV

UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class)

188. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully alleged herein.

189. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of providing wagers to Defendant for gambling and by providing their valuable PII to Defendant.

190. Plaintiff and Class Members provided Defendant their PII with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. In exchange, Plaintiff and Class members should have received adequate protection and data security for such PII held by Defendant.

191. Defendant benefited from receiving Plaintiff's and Class Members' payments for services and from receiving their PII through its ability to retain and use that information for its own benefit. Defendant understood and accepted this benefit.

192. Defendant knew Plaintiff and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

193. Defendant also understood and appreciated that Plaintiff's and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

194. Defendant failed to provide reasonable security, safeguards, and protections to the PII of Plaintiff and Class Members.

195. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff' and Class Members' PII.

196. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead made calculated decisions to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

197. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

198. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

199. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

200. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

201. Plaintiff and Class Members have no adequate remedy at law.

202. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury as described herein.

203. Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

COUNT V

INVASION OF PRIVACY
(On Behalf of Plaintiff and the Nationwide Class)

204. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully alleged herein.

205. Plaintiff and Class Members had a legitimate expectation of privacy regarding their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

206. Defendant owed a duty to Plaintiff and Class Member to keep their PII confidential.

207. The unauthorized disclosure and/or acquisition (*i.e.*, theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person.

208. Defendant's reckless and negligent failure to protect Plaintiff's and Class Members' PII constitutes an invasion of privacy by unreasonable publication of private facts about Plaintiff and Class Members—facts of a kind that would be highly offensive to a reasonable person.

209. Defendant's failure to protect Plaintiff's and Class Members' PII acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

210. Defendant knowingly did not notify Plaintiff and Class Members in a timely fashion about the Data Breach.

211. Because Defendant failed to properly safeguard Plaintiff's and Class Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

212. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

213. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII is still maintained by Defendant with their inadequate cybersecurity system and policies.

214. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

215. Plaintiff, on behalf of himself and Class Members, seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' PII.

216. Plaintiff, on behalf of himself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT VI

VIOLATION OF NEW JERSEY CONSUMER FRAUD ACT (NJCFA)
(On Behalf of Plaintiff and the Nationwide Class, or alternatively, the New Jersey Subclass)

217. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully alleged herein.

218. Plaintiff brings this claim on behalf of himself and the Nationwide Class, or alternatively, the New Jersey Subclass.

219. The New Jersey Consumer Fraud Act makes unlawful "[t]he act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing concealment, suppression or omission of any material fact with the intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby." N.J. STAT. ANN. § 56:8-2.

220. By the acts and conduct alleged herein, Defendant committed unfair or deceptive acts and practices by:

a. failing to maintain adequate computer systems and data security practices to safeguard PII;

b. failing to disclose that its computer systems and data security practices were inadequate to safeguard PII from theft;

c. the continued gathering and storage of PII, and other personal information after Defendant knew or should have known of the security vulnerabilities of its computer systems that were exploited in the data breach; and,

d. the continued gathering and storage of PII, and other personal information after Defendant knew or should have known of the Data Breach and before Defendant allegedly remediated the data security incident.

221. These unfair acts and practices violated duties imposed by laws including, but not limited to, the Federal Trade Commission Act and the NJCFA.

222. The foregoing deceptive acts and practices were directed at New Jersey consumers/purchasers and other consumers nationwide.

223. Defendant, Plaintiff, and Class Members are "persons" within the meaning of N.J. STAT. ANN. § 56:8-1(d).

224. Defendant engaged in "sales" of "merchandise" within the meaning of N.J. STAT. ANN. § 56:8-1(c), (d).

225. The foregoing deceptive acts and practices are misleading in a material way because they fundamentally misrepresent the character of the gambling services provided, specifically as to the safety and security of PII, and other personal and private information, to induce consumers to place wagers and/or bets at MGM.

226. Defendant's unconscionable commercial practices, false promises, misrepresentations, and omissions set forth in this Complaint are material in that they relate to matters which reasonable persons, including Plaintiff and members of the Class, would attach importance to in making their gambling decisions or conducting themselves regarding their gambling at MGM.

227. Plaintiff and Class Members are consumers who placed bets and/or wagers at MGM for the furnishing of gambles that were primarily for personal, family, or household purposes. And Defendant conducts its' business in New Jersey, where it is headquartered to consumers in New Jersey, New York, and throughout the United States.

228. Defendant engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, consumers placing bets and/or wagers, including Plaintiff and Class Members. Defendant's acts, practices, and omissions were done in the course of Defendant's business of marketing, offering to sell, and furnishing gambling services to consumers in the State of New Jersey. As a direct and proximate result of Defendant's multiple, separate violations of N.J. STAT. ANN. § 56:8-2,

229. Plaintiff and Class Members were injured because: (a) they would not have gambled at Defendant had they known the true nature and character of Defendant's data security practices; (b) Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of promises that Defendant would keep their information reasonably secure; and (c) Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

230. Plaintiff and the Class Members suffered damages including, but not limited to: (i) their financial accounts and funds within such being frozen; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Class; and (vii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

231. As a result, Plaintiff and the Class Members have been damaged in an amount to be proven at trial.

232. Also as a direct result of Defendant's violation of the New Jersey Consumer Fraud Act, Plaintiff and the Class Members are entitled to damages and injunctive relief, including, but not limited to, ordering Defendant to: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

233. On behalf of himself and other members of the Class, Plaintiff is entitled to recover legal and/or equitable relief, including an order enjoining Defendant's unlawful conduct, treble damages, costs, and reasonable attorneys' fees pursuant to N.J. STAT. ANN. § 56:8-19, and any other just and appropriate relief.

COUNT VII

VIOLATIONS OF THE TRUTH-IN-CONSUMER CONTRACT, WARRANTY, AND NOTICE ACT ("TCCWNA") (N.J.S.A. § 56:12-15) (On Behalf of Plaintiff and the Nationwide Class, or alternatively, the New Jersey Subclass)

234. Plaintiff incorporates by reference the preceding paragraphs as if fully set forth herein.

235. Plaintiff brings this Count on behalf of himself and the Nationwide Class, or alternatively, the New Jersey Subclass.

236. Plaintiff and Class Members are "consumers" within the meaning of N.J.S.A. § 56:12-15.

237. Defendant is a "seller" within the meaning of N.J.S.A. §§ 56:12-15 and -17.

238. Defendant violated the TCCWNA with respect to Plaintiff and the Class involving in Defendant's Data Breach by violating the CFA, as alleged above and in Count VI. Thus, Defendant violated Plaintiff's and the Class Members' clearly established legal rights or responsibilities of Defendant under the CFA and, therefore, Defendant violated the TCCWNA.

239. As a result of Defendant's violations of the TCCWNA, Plaintiff and those similarly situated are entitled to statutory damages of not less than $100 for each of Defendant's TCCWNA violations, as provided by N.J.S.A. § 56:12-17.

COUNT VIII
VIOLATIONS OF NEW YORK CONSUMER LAW FOR DECEPTIVE ACTS AND PRACTICES (GBL)
(N.Y. Gen. Bus. Law § 349)
(On Behalf of the New York Subclass)

240. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully alleged herein.

241. Plaintiff brings this Count on behalf of himself and the New York Subclass members.

242. New York General Business Law ("NYGBL") § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

243. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of the NYGBL § 349. The conduct alleged herein is a "business practice" within the meaning of the NYGBL § 349, and the deception occurred within New York State. Defendant stored Plaintiff's and the Class members' PII in Defendant's electronic and consumer information databases. Defendant knew or should have known it did not employ reasonable, industry standards, and appropriate security measures that complied "with federal regulations" and that would have kept Plaintiff's and the Class members' PII secure and prevented the loss or misuse of Plaintiff's and the Class members' PII. Defendant did not disclose to Plaintiff and the Class members that its data systems were not secure.

244. Plaintiff and the Class would never have gambled at BetMGM and provided their sensitive and personal PII to Defendant if they had been told or knew that Defendant failed to maintain sufficient security to keep such PII from being hacked and taken by others, and that

Defendant failed to maintain the information in encrypted form. Defendant violated the NYGBL §349 by misrepresenting, both by affirmative conduct and by omission, the safety of Defendant's many systems and services, specifically the security thereof, and its ability (or lack thereof) to safely store Plaintiff's and the Class members' PII.

245. Defendant also violated NYGBL §349 by failing to implement reasonable and appropriate security measures or follow industry standards for data security, and by failing to immediately notify Plaintiff and the Class members of the Data Breach. If Defendant had complied with these legal requirements, Plaintiff and the other Class members would not have suffered the damages related to the Data Breach as alleged herein.

246. Defendant's practices, acts, policies and course of conduct violate NYGBL § 349, *inter alia*, in that:

a. Defendant actively and knowingly misrepresented or omitted disclosure of material information to Plaintiff and the Class at the time they provided such PII that Defendant did not have sufficient security or mechanisms to protect PII;

b. Defendant failed to give timely warnings and notices regarding the defects and problems with its system(s) of security systems that they maintained to protect defects in its IT systems and failed to address the same or to give timely warnings that there had been a Security Breach.

247. Plaintiff and the Class were entitled to assume, and did assume, Defendant would take appropriate measures to keep their PII safe. Defendant did not disclose at any time that Plaintiff's and the Class's PII was vulnerable to hackers because Defendant's data security measures were inadequate, and Defendant was the only one in possession of that material information, which it had a duty to disclose.

248. The aforementioned conduct is and was deceptive, false, and fraudulent and constitutes an unconscionable commercial practice in that Defendant has, by the use of false or

deceptive statements and/or knowing intentional material omissions, misrepresented and/or concealed the defective security system they maintained and failed to reveal the Data Breach timely and adequately.

249. Members of the public were deceived by and relied upon Defendant's affirmative misrepresentations and failures to disclose.

250. Such acts by Defendant are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer providing his or her PII to Defendant. Said deceptive acts and practices are material. The requests for and use of such PII in New York through deceptive means occurring in New York were consumer-oriented acts and thereby falls under the New York consumer fraud statute, NYGBL § 349.

251. Defendant's wrongful conduct caused Plaintiff and the Class to suffer a consumer-related injury by causing them to incur substantial expense to protect from misuse of the PII materials by unauthorized third parties and cybercriminals and placing the Plaintiff and the Class at serious risk for monetary damages.

252. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class members suffered damages as alleged above.

253. In addition to or in lieu of actual damages, because of the injury, Plaintiff and the Class seek statutory damages for each injury and violation which has occurred.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a. For an Order certifying the Class, as defined herein, and appointing Plaintiff and his Counsel to represent the Class;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any

accurate disclosures to Plaintiff and Class Members;

c. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

xvii. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

xviii. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

xix. For prejudgment interest on all amounts awarded; and

xx. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Jury trial is demanded by Plaintiff and members of the putative Class.

Date: January 20, 2023

Respectfully Submitted,

LAUKAITIS LAW FIRM LLC

s/ Kevin Laukaitis
Kevin Laukaitis (NJ Bar ID # 155742022)
737 Bainbridge Street #155
Philadelphia, PA 19147
Phone: 215-789-4462
Email: klaukaitis@laukaitislaw.com

Attorneys for Plaintiff and the Proposed Classes